Volume 2, Issue 4, April 2012 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Scheme for Secure Image Transmission using ECC over the Fraudulence Network

Shubhi Gupta*
M.Tech. Scholar, Deptt. of C.S.E., K.E.C., Ghaziabad, U.P. India
sr23.shubhi@gmail.com

P.S. Gill
Professor, Deptt. of C.S.E., K.E.C., Ghaziabad, U.P. India

Awakash Mishra
Deptt. of MCA, R.K.G.E.C, Ghaziabad, U.P. India

Abhishek Dwivedi
Deptt. of MCA, R.K.G.E.C, Ghaziabad, U.P. India

*Abstract- **The requirement of secure transmission of data is important in our life. The transmission should be more secure when channel/network is too noisy/fraudulent. Image transmission is one of the application that must be securely transmitted over the fraudulence network. Secure transmission of image is required in various fields like medical/telemedicine, military etc. In this paper, we introduce a new scheme for secure transmission of medical image over the fraudulence network. Our approach is a combination of cryptography, and compression with removal of transmission errors. Cryptography provides secure transmission, Compression increases the capacity of transmission channel and Fuzzy is used for error which gets during transmission of image.***

Keywords - ECC public key cryptosystem, Image, Compression, Error Detection & Correction.

I. INTRODUCTION

Cryptography is the practice and study of techniques for secure communication. Cryptography is a branch of applied mathematics that aims to add security in the ciphers of any kind of messages. Cryptography algorithms use encryption keys, which are the elements that turn a general encryption algorithm into a specific method of encryption. The data integrity aims to verify the validity of data contained in a given document. [1]

To reduce the size of sending files, a compression scheme can be employed what is known as lossless compression on secrete message to increase the amount of hiding secrete data, a scheme that allows the software to exactly reconstruct the original message [2].

The transmission of numerical images often needs an important number of bits. This number is again more consequent when it concerns medical images. If we want to transmit these images by network, reducing the image size is important. The goal of the compression is to decrease this initial weight. This reduction strongly depends of the used compression method, as well as of the intrinsic nature of the image. Therefore the problem is the following:

1. To compress without lossy, but with low factor compression. If you want to transmit only one image, it is satisfactory. But in the medical area these are often sequences that the doctor waits to emit a diagnostic.

2. To compress with losses with the risk to lose information. The question that puts then is what the relevant information is to preserve and those that can be neglected without altering the quality of the diagnosis or the analysis. The human visual system is one of the means of appreciation, although subjective and being able to vary from an individual to another. However, this system is still important to judge the possible causes of degradation and the quality of the compression [3].

In this paper, we introduce an effective approach to transmit a secure and compressed image over fraudulent transmission channel. The organization of the paper is sketched as follows. In section 2, a necessary background and a brief remark is given. In section 3, we present the effective scheme based on ECC. In section 4, the security analysis of the proposed scheme is given, and we give some conclusions in section 5.

II. PRELIMINARIES

A- The ECC Public-Key Cryptosystem:

Elliptic Curve Cryptography (ECC) [4, 5] is a public key cryptography. In public key cryptography, each user or the device taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. The mathematical operations of ECC is defined over the elliptic curve $y^2 = x^3 + ax + b$, where $4a^3 + 27b^2 \neq 0$.

Each value of the 'a' and 'b' gives a different elliptic curve. All points (x, y) which satisfies the above equation plus a point at infinity lies on the elliptic curve. The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator point G in the curve. The generator point G, the curve parameters 'a' and 'b', together with few more constants constitutes the domain parameter of ECC.

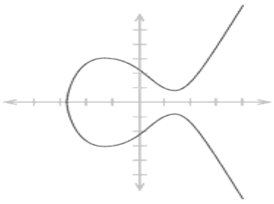

Figure1: An Elliptic curve.

Operation

For curve $y^2 = x^3 + ax + b$

1. Elliptic Curve Point Addition.
- Point Addition $P(x_1,y_1) \neq Q(x_2,y_2)$.
- Point Doubling $P(x_1,y_1)$

2. Elliptic Curve Scalar Multiplication.
- It computes k×P for a given point P and integer k. Q = k×P = (P + P + … + P) ((k-1) addition)

Elliptic Curve Cryptosystem [6]

1. Bob chooses the curve E and point P on the curve
2. Bob chooses integer d and calculates Q = d×P and makes it public
3. Alice maps the plaintext m to point M on curve
4. Alice chooses a random integer k
5. Alice encrypts M as $C_1 = k\times P$, $C_2 = M + k\times Q$
6. Bob decrypts by calculating $M = C_2 - d\times k\times P$
7. $M = C_2 - d\times k\times P = M + k\times Q - d\times k\times P = M + k\times Q - d\times Q = M$.

B- The SEQUITUR Algorithm

The SEQUITUR algorithm [7] represents a finite sequence _ as a context free grammar whose language is the singleton set {σ}. It reads symbols one-by-one from the input sequence and restructures the rules of the grammar to maintain the following invariants:

- no pair of adjacent symbols appear more than once in the grammar, and
- every rule (except the rule defining the start symbol) is used more than once.

To intuitively understand the algorithm, we briefly describe how it works on a sequence 123123. As usual, we use capital letters to denote non-terminal symbols. After reading the first four symbols of the sequence 123123, the grammar consists of the single production rule S ➔ 1, 2, 3, 1 where S is the start symbol. On reading the fifth symbol, it becomes S ➔ 1, 2, 3, 1, 2 Since the adjacent symbols 1, 2 appear twice in this rule (violating the first invariant), SEQUITUR introduces a non-terminal A to get

S ➔ A, 3,A A ➔1, 2

Note that here the rule defining non-terminal A is used twice. Finally, on reading the last symbol of the sequence 123123 the above grammar becomes

S ➔ A, 3, A, 3 A ➔ 1, 2

This grammar needs to be restructured since the symbols A, 3 appear twice. SEQUITUR introduces another non-terminal to solve the problem. We get the rules

S ➔ B,B B ➔ A 3 A➔ 1 2

However, now the rule defining non-terminal A is used only once. So, this rule is eliminated to produce the final result.

S ➔ B, B B ➔ 1, 2, 3

Note that the above grammar accepts only the sequence 123123.

C- Block Error Rate:

The application's block error rate can be computed from the bit error rate using the following equation [8]:

$$BLER = \binom{N}{E} * P^E * (1 - P)^{N-E}$$

Where: N is the number of bits in a block, E is the number of errors in a block and p is the probability of a bit error (bit error rate)

This equation basically states that the block error rate is dependent on three factors:

• The number of statistical combinations of failing bit patterns (E combinations of N),

• The probability of E errors occurring (*p* raised to the E power), and

• The probability of N-E correct data bits ((1-*p*) raised to the N-E power).

D- Error Correction Code:

A metric space is a set C with a distance function dist : $C \times C \rightarrow R^+ = [0,\infty)$, which obeys the usual properties(symmetric, triangle inequalities, zero distance between equal points) [9, 10].

Definition: Let $C\{0,1\}^n$ be a code set which consists of a set of code words c_i of length n. The distance metric between any two code words c_i and c_j in C is defined by

$$dist(c_i, c_j) = \sum_{r=1}^{n} |c_{ir} - c_{jr}| \qquad c_i, c_j \in C$$

This is known as Hamming distance [11].

Definition: An error correction function f for a code C is defined as $f(c_i) = \{c_j \,/\, dist(c_i, c_j) \text{ is the minimum, over } C - \{c_i\}\}$. Here, $c_j = f(c_i)$ is called the nearest neighbour of c_i [9].

Definition: The measurement of nearness between two code words c and c' is defined by $nearness(c,c') = dist(c,c')/n$, it is obvious that $0 \le \text{nearness } (c,c') \le 1$[11].

Definition: The fuzzy membership function for a codeword c' to be equal to a given c is defined as [11]

$$FUZZ(c') = 0 \qquad \text{if nearness}(c,c') = z \le z_0 < 1$$
$$= z \qquad \text{otherwise}$$

III. Our Scheme

A complete transmission process includes the following steps: [12]

Step 1: Generating $n \times n$ *blocks:*

In RGB space the image is split up into red, blue and green images. The image is then divided into 8×8 blocks of pixels and accordingly the image of $w \times h$ pixels will contain $W \times H$ blocks. Where, $W = w/8$, $H = h/8$.

Step 2: DCT:

All values are level shifted by subtracting 128 from each value. The Forward Discrete Cosine Transform of the block is then computed. The mathematical formula for calculating the DCT is:

$$T(u,v) = \sum_{x=0}^{n}\sum_{y=0}^{n} f(x,y).\, g(x,y,u,v)$$

Where,

$$g(x,y,u,v) = \frac{1}{4}\alpha(u)\,\alpha(v)\cos\left[\frac{(2x+1)u\pi}{2n}\right]\cos\left[\frac{(2y+1)v\pi}{2n}\right]$$

Where

$$\alpha(u) = \begin{cases} \frac{1}{\sqrt{2}} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots .for.u = 0 \\ 1 \ldots\ldots\ldots\ldots\ldots\ldots\ldots .for.u = 1,2,\ldots.N-1 \end{cases}$$

Step 3: Quantization:

Quantization is the step where the most of the compression takes place. DCT really does not compress the image, as it is almost lossless. Quantization makes use of the fact that, the high frequency components are less important than the low frequency components. The Quantization output is

$$Q_{DCT} = round\left(\frac{T(u,v)}{Z(u,v)}\right)$$

The $Z(u,v)$ matrix could be anything, but the JPEG committee suggests some matrices which work well with image compression.

Step 4: Compression using SEQUITUR:

After quantization, the scheme uses a filter to pass only the string of non-zero coefficients. By the end of this process we will have a list of non-zero tokens for each block preceded by their count.

DCT based image compression using blocks of size 8x8 is considered. After this, the quantization of DCT coefficients of image blocks is carried out. The SEQUITER compression is then applied to the quantized DCT coefficients.

The compression achieved in this approach is evaluated based on the overall compression ratio (CR) which is defined as:

$$\text{C.R.} = \frac{\textit{size of the input or original image}}{\textit{sizeof output or compressed image}}$$

Step 5: Encryption using ECC:

In encryption phase, ECC takes the output of compression phase as a message as a plaintext.

Decryption Process is the inverse step of encryption process.

Step 6, 7: Error Detection and Correction:

If any error occurred during the transmission, Receiver check that $dist(t(c)c') > 0$, he will realize that there is an error occurs during the transmission. Receiver apply the error correction function f to $c' : f(c)$.

Then receiver will compute

nearness $(t(c), f(c')) = dist(t(c) f(c'))/n$

$$FUZZ(c') = 0 \qquad \text{if nearness}(c,c') = z \le z_0 < 1$$
$$= z \qquad \text{otherwise}$$

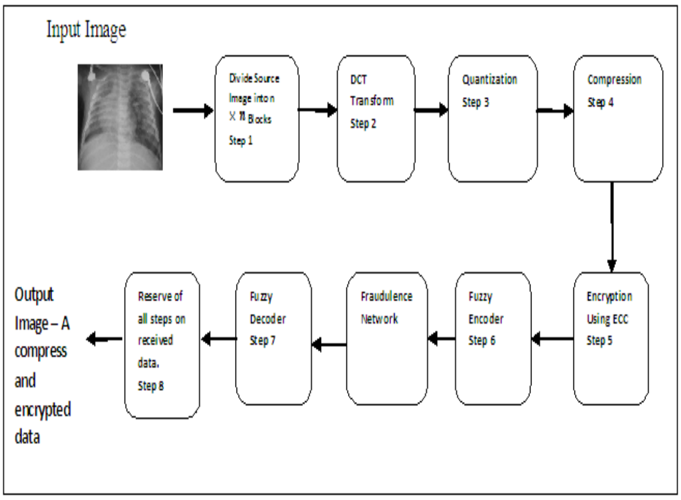
Input Image
Divide Source Image into n X n Blocks Step 1
DCT Transform Step 2
Quantization Step 3
Compression Step 4
Encryption Using ECC Step 5
Fuzzy Encoder Step 6
Fraudulence Network
Fuzzy Decoder Step 7
Reserve of all steps on received data. Step 8
Output Image – A compress and encrypted data

Figure 2: Architecture of Proposed Scheme.

IV. Security Analysis

In this proposed scheme we use ECC Cryptosystem to make secure image transmission over the fraudulence network, because ECC is one of the public key cryptosystem that provides same level of security with smaller keys. By using Compression technique with sequitur algorithm and Error correction code with ECC cryptosystem we get highly secured data.

We verified that the compression ratio of Sequitur outperforms Gzip as well as Compress. On the other hand, however, the compression and decompression are very slow compared to Gzip and Compress, because Sequitur utilizes the arithmetic coding that is time consuming, and the program might not be fully optimized. From our view point of compressed pattern matching, compression time is not a serious matter, while the decompression time is critical. In the original program of Sequitur, decompression routine borrows the same data structures, such as doubly linked list, that are unnecessary for decompression only. Thus we simply rewrote the decompression routine using a standard array.

When the encoded message *c* is transmitted. It is possible that during the transmission some bits of c can be changed and the receiver receives the incorrect message *c'*. He calculates that *dist*(*x*, *y*) is minimum. If the error is not too large, that is $\mathrm{dist}(c, c') < \frac{1}{2d}$, where d is the minimum distance of any two distinct code words, then *c'* is equal to the original message *c*.

V. CONCLUSION

In this paper, we present the ECC based secure and efficient scheme for Image transmission. Our scheme provides the complete security and compressed form of image over the fraudulence network, which provides the maximum efficiency to transmission channel. If any error is occurred by channel, the fuzzy error correction code removes the error and provides the more perfect image to the receiver.

REFERENCES

[1] Diego F. de Carvalho, Rafael Chies, Andre P. Freire, Luciana A. F. Martimiano and Rudinei Goularte, "Video Steganography for Confidential Documents: Integrity, Privacy and Version Control" , University of Sao Paulo – ICMC, Sao Carlos, SP, Brazil, State University of Maringa, Computing Department, Maringa, PR, Brazil.

[2] Nameer N. EL-Emam, "Hiding a Large Amount of Data with High Security Using Steganography Algorithm" Applied Computer Science Department, Faculty of Information Technology, Philadelphia University, Jordan

[3] Borie J., Puech W., and Dumas M., "Crypto-Compression System for Secure Transfer of Medical Images", 2nd International Conference on Advances in Medical Signal and Information Processing (MEDSIP 2004), September 2004.

[4] Certicom, Standards for Efficient Cryptography, SEC 1: Elliptic Curve Cryptography, Version 1.0, September 2000.

[5] Certicom, Standards for Efficient Cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters, Version 1.0, September 2000.

[6] A. Hosseinzadeh Namin, Elliptic Curve Cryptography, RESEARCH CENTRE FOR INTEGRATED MICROSYSTEMS–UNIVERSITY OF WINDSOR, April 2005.

[7] N.Walkinshaw, S.Afshan, P.McMinn "Using Compression Algorithms to Support the Comprehension of Program Traces" Proceedings of the International Workshop on Dynamic Analysis (WODA 2010) Trento, Italy, July 2010.

[8] http://www.fcet.staffs.ac.uk/alg1/2004_5/Semester_1/Communications,%20COMMS%20(CE00038-2)/word%20notes/Block%20Error%20Rate.doc

[9] J.P.Pandey, D.B.Ojha, Ajay Sharma, "Enhance Fuzzy Commitment Scheme: An Approach For Post Quantum Cryptosystem", in Journal of Applied and Theoretical Information Technology, (pp 16-19) Vol. 9, No. 1, Nov. 2009.

[10] V.Pless, " Introduction to theory of Error Correcting Codes", Wiley , New York 1982.

[11] A.A.Al-saggaf,H.S.Acharya,"A Fuzzy Commitment Scheme"IEEE International Conference on Advances in Computer Vision and Information Technology 28-30November 2007 – India

[12] G. Lo-varco,W. Puech, and M. Dumas. "Dct-based watermarking method using error correction codes", In ICAPR'03, International Conference on Advances inPattern Recognition, Calcutta, India, pages 347–350, 2003.